附件 7

“网络空间安全治理”重点专项 2023 年度项目申报指南及“揭榜挂帅”榜单

（仅国家科技管理信息系统注册用户登录可见）

为落实“十四五”期间国家科技创新有关部署安排，国家重点研发计划启动实施“网络空间安全治理”重点专项。根据本重点专项实施方案的部署，现发布 2023 年度项目申报指南。

本重点专项总体目标是：围绕全球网络公害、涉及民生的数据资产和“新基建”基础设施等领域的安全挑战，开展互联网基础设施、数据、网络公害、新技术新应用领域安全治理的战略性、基础性、前沿性研究，到 2025 年力争打造自立自强的网络空间安全治理技术体系，形成中国特色的网络空间安全治理方案，支撑实现网络空间的“共建、共治、共享”。

2023 年度指南部署坚持问题导向、分步实施、重点突出的原则，围绕互联网基础设施治理、网络空间数据治理、网络公害与内容治理、新技术新应用治理 4 个技术方向，按照基础研究、共性关键技术两个层面，拟启动 19 项指南任务，拟安排国拨经费 2.28 亿元。其中，围绕互联网基础设施治理、网络空间数据治理、网络公害与内容治理等技术方向，部署青年科学家项目，每个项目 200 万元。青年科学家项目对配套经费不做要求，可不要求指

南内容全覆盖。共性关键技术类项目配套经费与国拨经费比例不低于 1.5:1。项目由相关专业机构组织，采用专家评审、第三方权威机构测评或用户部门试用评价等方式开展考核。

项目统一按指南二级标题（如 1.1）的研究方向申报。除特殊说明外，每个方向拟支持项目数为 1 项，实施周期不超过 3 年。申报项目的研究内容必须涵盖二级标题下指南所列的全部研究内容和考核指标。基础研究类项目下设课题不超过 4 个，项目参与单位总数不超过 6 家；共性关键技术类项目下设课题数不超过 5 个，项目参与单位总数不超过 10 家。项目设 1 名项目负责人，项目中每个课题设 1 名课题负责人。

青年科学家项目不要求对指南内容全覆盖，不再下设课题，项目参与单位总数不超过 3 家。项目设 1 名项目负责人，青年科学家项目负责人年龄要求，男性应为 1985 年 1 月 1 日以后出生，女性应为 1983 年 1 月 1 日以后出生。原则上团队其他参与人员年龄要求同上。

1 互联网基础设施治理

1.1 互联网域名服务授权机制的安全模型分析与安全增强技术（基础研究类，青年科学家项目）

研究内容: 针对互联网域名解析体系中重要域名授权依赖信任链冗长、易被攻击者隐蔽劫持操控的问题: 研究域名系统授权机制的安全威胁建模方法，提出脆弱性分析技术；研究重要域名及其海量子域名授权依赖关系安全状态的快速评估技术；研究基于域名系

统复杂授权的网络攻击行为发现及风险预警技术;研究兼容国际域名协议标准的轻量级域名系统授权机制安全增强技术。

考核指标：提出域名系统授权机制的安全威胁建模方法，面向 BIND 软件在内的不少于 8 款主流域名解析软件，以及不少于 40 家重要域名解析厂商，完成脆弱性分析，向中国国家漏洞数据库（CNVD）提交不少于 10 个相关安全漏洞；具备百万级重要域名与千万级子域名的授权依赖安全状态风险评估能力，且评估时间不大于 4 小时；提出基于域名系统复杂授权的网络攻击风险发现模型，风险预警准确率不低于 95%；提出通用轻量级域名授权机制安全增强技术，域名解析服务整体性能下降不超过 5%。

有关说明：拟支持 2 项。

关键词：域名系统安全，域名授权威胁，域名安全增强。

1.2 基于我国标准密码算法的实时可信身份技术及其应用（共性关键技术类）

研究内容：面向多网融合场景下时间敏感应用的可信身份认证需求，研究高可信实时身份保障框架，构建新型身份信任网络基础系统；研究开放环境下基于我国标准密码算法的实时身份可信主体要素模型，实现基于基础信任源的端到端可信安全身份基的构建，实现身份全网安全可证明与验证；研究跨异构网/域的高效实时身份认证链传递模型，实现可信身份机制与业务协议有机的融合，提供多层次、多场景可信身份服务；研究基于我国标准密码算法的实时身份泛在关键密码技术，实现轻量级、低成本、

可扩展的弱计算能力通信终端的密钥管理、签名验签等可信身份相关密码功能；针对广泛使用的电话通信等典型应用场景，研究实时可信身份系统支撑技术，构建完整的产品技术链，包括可信身份管理、运维支撑和监测监督等技术，并进行规模化应用验证。

考核指标：研究开放环境下的实时可信身份保障体系框架，搭建支持端到端可信身份验证的基础系统，具备跨地域、跨网络的多层次可信身份信任的快速构建、可证明与验证管理能力，跨异构网络的端到端身份证明与验证时间不大于300ms，核心网络网关到网关的鉴别延时不大于200ms，具备全面支持我国标准密码算法，包括SM2，SM3、SM4和SM9算法；完成至少1项面向商用非定制终端的安全人机绑定技术，具备抗设备丢失的身份安全能力；完成至少2款支持会话初始协议（SIP）通信的可信终端，2款支持4/5G并支持SIP的移动智能终端通信可信模块，1款可信通信网关产品研制；完成不少于3个省级示范应用，可信身份服务能力不少于1亿，月有效呼叫累计次数不少于1000万，支持不少于2类典型应用场景；研制的身份运维支撑系统应能自动对接我国的实名身份认证系统和许可的数字证书认证系统，身份证明信息转发速度不小于1千万次/秒；至少完成2份互联网工程任务组（IETF）标准草案或国家或行业标准立项。

关键词：可信身份，实时，密码，通信。

1.3 分布式无证书网络身份系统的关键技术（共性关键技术类）

研究内容：针对传统身份认证系统证书管理复杂，中心化身

份认证效率低、受网络攻击风险大，无法满足海量异构物联网终端和节点安全可靠接入的身份认证需求，研究基于精确时标和位置信息的抗攻击共识算法，设计基于区块链的高性能无证书的网络身份认证系统架构；研究在密钥安全性无法持续保障时安全可靠的身份认证协议及基于区块链的无证书认证系统的密钥管理协议，保障物联网设备认证的高效安全性；研究支持海量物联网终端身份认证协议的硬件加速方案，突破大规模终端并发接入时分布式认证的效率瓶颈；研究适用于海量异构物联网节点身份认证的高性能智能合约虚拟机技术，解决制约大规模区块链智能合约并发执行的计算能力问题；研究大规模分布式数字身份系统集成与应用方案，构建基于国产芯片的分布式大规模物联网身份认证基础设施，面向典型行业开展技术应用验证。

考核指标：提出高性能分布式无证书网络身份认证体系架构；设计分布式环境下无证书的网络身份认证协议族，满足密钥安全性无法持续保障时对身份信息的可靠验证，实现基于区块链的无证书认证系统的密钥生成、密钥分发、密钥回收等；基于国产芯片的服务器平台，研发一套高性能分布式无证书的网络身份认证系统；基于精确时标和位置信息的抗攻击共识算法事务处理量达到每秒 5 万次以上；硬件加速国密身份认证计算性能达每秒 10 万次以上，单节点支持 10 万个以上物联网终端并发安全链接；通过硬件加速可承载每秒 50Gbit 以上物联网终端认证流量；单节点的身份认证哈希计算能力达每秒 100Gbit 以上，以支持高效和

全程可溯源的区块链身份认证；身份认证区块链网络至少 4 个主节点；在至少 2 个典型工业互联网等场景开展示范验证。

关键词：分布式身份认证，无证书，区块链。

2 网络空间数据治理

2.1 基于完备代数群模型的隐私保护基础理论（基础研究类，青年科学家项目）

研究内容：面向数据安全领域中关于数据隐私保护的相关任务，围绕数据安全流通和使用及保障隐私数据个人权益场景中对高性能隐私保护技术的需求，研究基于零知识证明的隐私保护技术及其在密码学领域可证明安全框架下的理论基础——代数群模型；针对多项隐私保护技术的理论基础（代数群模型）被证伪，进而引发的相关隐私保护技术出现广泛安全风险的问题，分析代数群模型的严格定义方法，推进代数群模型完备化的基础性研究，突破基于代数群模型的相关隐私保护技术在可证明安全框架下的技术瓶颈，完成多项工业界隐私保护技术在完备的代数群模型下的安全性形式化验证。

考核指标：所重构的代数群模型在密码学领域可证明安全框架下具有完备性，可以支撑基于该模型的隐私保护技术可证明安全的功能；提出基于完备代数群模型的隐私保护技术的通用性形式化验证方案 1 项；所提出的形式化验证方法能够对至少 5 项工业界隐私保护技术实现在完备代数群模型下安全性验证；完成相关专利 1 项和技术报告 2 篇。

有关说明：拟支持 2 项。

关键词：隐私保护技术，数据安全，代数群模型。

2.2 全同态加密关键密码算法及可信性验证方法（基础研究类，青年科学家项目）

研究内容：围绕数据安全保护场景中对密态计算的需求，研究基于整格及模格的全同态加密算法及加密体系转换方法，形成统一的计算误差分析理论及安全性评估技术；研究全同态算法自动构成理论及同态算法中间表示，形成由明文算法向同态算法的自动编译框架；研究全同态加密计算验证理论，形成对全同态算法的可信性验证技术；融合以上理论、方法和技术，形成新型全同态加密算法及可信性验证理论体系，并应用于机器学习、数据分析等领域，形成全栈式全同态加密理论验证平台。

考核指标：提出统一的计算误差分析理论与安全性评估技术，能够对融合整格、理想格及模格等 3 种以上加密体系的全同态算法进行计算误差分析与安全性评估，分析误差与实际误差之间相差不超过 0.0002%；基于自主研发的开源全同态加密计算平台，实现全同态机器学习算法及全同态数据库算法的自动编译；支持在恶意环境中对密文上执行的全同态算法进行验证，验证计算的额外时间开销低于原计算时间的 20%；支持包括残差网络（ResNet-50）在内的不少于 3 种以上的机器学习模型推理计算，在加拿大高级研究所-10（CIFAR-10）数据集上的平均推理精度不低于 90%，在单核中央处理器（CPU）上对单张图像推理时计

算时间不高于400秒;在国产数据库系统中支持全加密数据过滤、聚合、排序等算法，支持16比特及以上数据的不限深度过滤及聚合，同时在96核CPU服务器上每1万行的商业智能计算测试（TPC-H）下过滤聚合基准计算时间不高于60秒。

有关说明：一流网络安全示范学院牵头申报，拟支持2项。需填写预申报书。

关键词：全同态加密，应用密码学，可信同态计算。

2.3 移动通信的云网端协同个人数据可信保护技术（共性关键技术类，定向择优）

研究内容：针对移动通信环境个人数据安全保护需求，研究网络赋能的云网端协同个人数据可信保护技术体系；研究移动终端使能的个人数据可信备份与恢复、应急可信删除、多副本可信删除、可信存储管理、多模态密文检索等技术，支持个人数据可信管理; 研究云侧控制的持续身份认证模型、数据协作可信授权、数据安全增量更新、数据使用知情管理等技术，支持个人数据可信访问；研究云侧平台的个人数据分类分级技术及平台自身的数据安全漏洞检测、监测、防护、审计技术，支持个人数据可信保障；研究移动网络设施支配的跨主体数据鉴权模型、个人数据流通模型、数据异常发现、取证和处置等技术，支持个人数据风险管控。

考核指标：研发移动终端安全插件，支持多主体身份凭证采集、数据流信息采集、数据管理使能控制、数据环境可信度量代

理等功能，支持多副本密文数据可信删除，准确率大于95%，支持不少于3种模态数据的密文检索，检索时间平均损耗小于15%；支持不少于3种行为生物特征的端对端模型持续认证，延迟小于1秒；云侧平台个人数据分类分级到3~5级，实现100%覆盖，云侧平台数据安全检测、监测、防护误报率低于0.3%，漏报率低于0.5%，网络协议流量解析还原准确率不低于99.99%；研制1套网络赋能的个人数据安全中台，支持个人数据的可信备份与还原、应急可信删除、数据鉴权、数据异常发现、数据取证和数据流阻断等功能，数据鉴权至少支持3种主体可信身份凭证，中台服务请求日均吞吐率达到亿级；所构建的云网端协同个人数据可信保护技术体系在5G手机、5G网络和云平台的典型应用场景中应用，终端规模不少于1万台，至少形成3项行业标准草案。

有关说明：由国资委组织推荐，由企业牵头申报，配套经费与国拨经费不低于3:1。

关键词：个人数据，可信管理，可信访问，可信保障。

2.4 基于安全标识的敏感数据出境安全风险评估和预警技术（共性关键技术类）

研究内容：针对敏感数据出境安全风险评估与预警问题，研究海量数据安全标识技术、出境数据机构主体溯源技术，有效解决敏感数据出境全链条溯源、违规追踪等难题；研究数据出境的风险发生机理、面向机构主体的敏感数据出境安全风险量化评估模型，研究安全风险动态评估技术，构建风险要素和安全事件库，

提出敏感数据出境安全风险量化评估指标体系；研究机构主体风险采集与报送机制、机构主体间的风险传播机制，研究敏感数据出境异常事件分析、多源风险融合预警等技术，实现敏感数据出境预警，支撑相关部门进行敏感数据出境监管和风险应急处理。

考核指标：跨境业务服务的数据安全标识技术具备可溯源海量数据安全标识、安全标识抗损毁能力，可支持敏感出境数据相关机构主体全链条溯源和违规追踪等功能，支持一般数据管理和重要数据集中管控 2 种场景及其交互，2 种场景的安全标识识别率不低于 80%与 90%；数据出境安全风险量化评估模型支持上述 2 种出境数据场景、不少于 30 项关键风险要素，并构建相应的风险要素和安全事件库；敏感数据出境异常行为分析技术的分析准确率不低于 95%，形成的敏感数据出境预警技术误报率不超过 25%。

关键词：数据安全标识，数据出境安全，敏感数据出境监管，风险评估，风险预警。

2.5 面向数据可信确权与交易的安全保障技术（共性关键技术类）

研究内容：针对数据交易中的权益控制困难、侵权行为隐蔽、全程监管缺失等问题，研究数据交易的流通安全模型，以及数据的权益登记、可信发布、可控交易、权益转移等技术，构建数据交易的安全流转技术体系；研究数据确权、资产转移等技术，建立数据可信确权与交付机制，支持数据资产保护；研究全流程的细粒度状态控制、流转管控、使用控制权限可信处置与迁移等技

术，支撑数据交易中的受控使用；研究数据流转的全流程存证与审计、证据交叉认证与融合分析、违规判定与溯源等监测技术，支持数据攸关方的权益保障；搭建数据交易权益保障的技术验证平台。

考核指标：提出数据确权的量化指标体系，支撑数据确权与侵权判定；提出数据交易安全流转技术体系，包含数据交易全流程的细粒度状态控制、数据流转管控、使用控制权限可信处置与迁移等机制，可以支撑数据流转中的受控使用、全流程存证与审计、违规判定与溯源等功能；支撑违规行为判定不少于 10 种、准确率不低于 90%、在万级规模用户场景下违规判定时间为分钟级；搭建数据交易权益保障技术验证平台，该平台支持万级用户、10 种以上类别和十亿条以上数据，支持数据确权、权益转移、流转管控、使用控制、取证溯源等功能验证，并在数据交易平台、典型行业等开展示范应用。

关键词：数据交易，可信确权，受控使用，流转管控。

3 网络公害与内容治理

3.1 面向暗网抑制的普适性安全理论研究（基础研究类，青年科学家项目）

研究内容：研究基于输入感知的网络空间暗网流量分析共性特征提取，构建普适性暗网流量分析模型；研究超点中极低占比暗网流量的实时识别方法，结合高斯核函数和多模态优化等先进理论，突破高速网络空间中轻量化暗网流量实时识别技术瓶颈；

研究基于熵率原理等经典理论的多网络全时域连接预测与量化普适方法，突破动态网络空间安全量化的核心理论；研究面向真实环境的暗网陷阱模型部署多目标优化技术；基于图挖掘的暗网协议脆弱性关联分析，研究暗网端到端反侦测溯源机制。

考核指标：设计满足高速网络暗网流量实时检测的不少于 2 个不同普适理论模型,包括暗网流量特征提取模型和实时识别模型等；支持不少于 15 种主流暗网流量类型的检测，准确率不低于 98%；海量流量数据采样支持流平均 1 比特存储的在线超点检测，精度不低于 98%；在真实网络高速场景中暗网流量占比不高于 0.1%的情况下对不少于 7 种业务类型的实际贝叶斯检测精度不低于 90%，响应时间不高于 0.2s，存储空间不高于 1MB；支持 20 个公开真实网络的全时域连接可预测和量化;支持真实网络暗网混淆协议下的陷阱技术，陷阱节点存活率不低于 95%；暗网的行为主体和隐藏服务器溯源数量不少于 10000 个，准确率不低于 95%。

有关说明：一流网络安全示范学院牵头申报，拟支持 2 项。需填写预申报书。

关键词：高速网络，暗网，共性特征，协议脆弱性。

3.2 面向终端的高隐蔽传播网络公害识别、取证和归因研究（基础研究类）

研究内容：针对网络空间目的性更强、危害性更大、抗网络流分析能力更强的网络诈骗、网络黑灰产、网络勒索、恶意软件等高隐蔽传播网络公害，聚焦其监管分析难、取证处置难、行为主体

溯源难等问题，研究高隐蔽网络公害活动的匿迹机理和传播方法；研究面向终端的高隐蔽公害跨域特征分析与恶意样本无感化取证方法；研究异构终端资源受限下的微蜜罐主动诱导与取证方法；研究基于终端侧和网络侧分析相融合的高级网络公害行为智能识别模型与方法；研究高隐蔽传播网络公害全链条分析与行为主体谱系归因方法，支持国家网信与执法部门开展高隐蔽公害治理。

考核指标：支持加密、伪装等不少于 4 种网络公害匿迹机理刻画；针对物联网、智能手机等资源受限终端，支持木马远控、数据勒索、漏洞利用等 5 种以上高隐蔽公害识别、取证与归因，支持公害的微蜜罐捕获、恶意代码检测、跨域通道检测、端网融合检测、行为体归因，支持国家网信、执法等相关单位开展高隐蔽公害治理；实现 X86、ARM 等 3 种以上架构微蜜罐仿真，支持固件、协议、程序等 5 种以上模拟，仿真设备型号 50 种以上、欺骗模板 50 种以上；实现固件、内核、进程等 3 类伪装驻留恶意代码检测，支持 iOS、安卓等系统中飞马（Pegasus）、捕食者间谍软件（Predator）、跟踪软件（Stalkerware）等高隐蔽间谍软件检测；能够感知终端侧模拟信号变化威胁，支持电磁、声音等 3 类跨域威胁检测，支持端侧硬件级的无感化检测取证；能够建立 10 种以上终端侧与网络侧威胁融合分析模型，综合检出精确率不低于 90%、未知公害检出率不低于 80%、误报率不超过 3%；公害主体的归因准确率不低于 90%。

关键词：高隐蔽传播网络公害，活动匿迹机理，带外分析，

无感化取证，微蜜罐取证。

3.3 超大规模网络中恶意流量跨域监管与智能处置（基础研究类）

研究内容：针对超大规模网络中恶意流量的监管效率不足和威胁处置能力缺失,研究面向恶意流量监管的全息动态评价机制，构建集网络测量、流量分析、跨域协同与溯源阻断为一体的恶意流量监管处置体系；研究基于可编程数据面的软硬件结合流量探针和主被动结合的跨域检测点部署优化方案，突破常数级时延、亚线性存储、高精度的流量检测技术瓶颈，实现千万级网络流的实时采样和多域协同测量；研究面向动态网络环境的强隐蔽性恶意流量应用及变种通信早期特征构建和识别方法，实现细粒度行为流量切分、稳定特征提取和早期行为流量精准识别；研究跨域恶意流量数据关联分析，设计预测性资源在线编排和基于知识迁移的未知恶意流量精准识别技术，实现百亿节点、千亿边的超大规模网络恶意流量多域协同分析；针对恶意流量跨域追踪和防御策略动态博弈困境，研究多种主动防御机制广泛协同的恶意流量牵引机制和动态优化防御策略，研究具备自适应性和高交互性的欺骗防御技术，实现威胁主体溯源和恶意流量有效阻断。

考核指标：支持 Tbps 级以上的城域网真实流量环境中恶意流量的检测与识别，支持规则可达 5000 万以上，识别时间不超过 2 秒，准确率不低于 90%；隐蔽恶意应用流量包括未知恶意流量识别准确率不低于 95%，支持恶意应用流量细粒度攻击行为识别，细粒

度攻击行为分析在动态网络环境下的行为识别准确率超过 90%；支持城域网级跨域节点不少于 300 个；支持至少 12 类恶意流量的溯源和阻断，包括勒索软件、僵尸网络、DDoS 攻击、手机恶意 APP、泄密流量、黑客攻击漏洞、恶意感染主机、VPN 隐藏流量、区块链中的恶意行为、DNS 恶意流量隧道、钓鱼和垃圾邮件等。

关键词：恶意流量检测，跨域协同，流量识别，智能处置。

3.4 基于群体认知的社交用户意图分析机理（基础研究类，青年科学家项目）

研究内容：研究网络社交媒体中网民情感认知机理、观点扭转成因、社交网络结构和个体认知特征对群体观点形成的交互机理；研究低资源场景下的跨语言、跨文化网民立场检测和观点分析技术，支持显式立场检测、隐式立场检测和立场证据挖掘；研究多模态交互式对话场景下情感表征、动态情感识别、情感反转预测和情绪原因推理技术；研究社交媒体群体用户特定语用环境下的意图测绘和意图分析技术。

考核指标：针对政治、经济、文化等不同领域的舆情事件，提出网民情感认知机理不少于 5 个；小样本条件下社交媒体用户立场检测准确率大于 80%，多于 5 轮交互对话场景下的动态情感分析准确率大于 85%，情绪原因推理准确率大于 85%；构建特定语用环境下网民群体的意图测绘体系，不少于 20 个意图类别，意图研判准确率大于 70%，零样本意图研判准确率大于 60%。

有关说明：拟支持 2 项。

关键词：认知机理，意图研判，立场检测，动态情感分析。

3.5 跨社交媒体网络舆情传播与效果评估技术（共性关键技术类）

研究内容：研究跨社交平台多粒度舆情传播指标体系与演化模型；研究多语言跨平台的网络舆情事件传播溯源技术和传播范围预测技术；研究情绪原因辅助增强的信息内容筛选技术、分众化易感群体识别技术与信息推荐技术；研究面向影响力最大化的传播策略生成技术与传播效果度量评估技术；在舆情分析监测、虚假信息治理等典型场景开展技术验证。

考核指标：获取境内外不少于 50 个主流网络媒体平台数据源信息；提出多粒度网络舆情传播指标体系 1 套，不少于 40 个维度；境内外网络舆情传播溯源准确率不低于 90%，网络舆情传播态势预测准确率不低于 65%，支持不少于中文、英文等 5 个语种；构建不少于 10 种信息传播策略，面向特定主题的信息传播受众覆盖率不低于 60%，构建一套不少于 30 维的舆情传播效果度量指标体系；研发具有自主知识产权的社交网络舆情传播平台 1 套，在国家相关部门开展技术验证。

关键词：网络舆情传播，跨域溯源，易感人群识别，传播效果评估。

3.6 网络空间认知与情报推理关键技术研究（共性关键技术类，定向择优）

研究内容：研究新一代网络空间地理学理论体系，解决建立

网络空间保卫非对称能力的科学问题；以地理图谱为理论支撑，研究基于网络空间要素、结构及演变关系的动态认知关键技术，研究网络空间节点隐藏标签挖掘技术，研究服务依赖性影响因素和脆弱性测度体系框架，实现网络空间对抗环境认知图谱构建，为开展国家重要网络资产安全保卫、打击网络犯罪提供关键技术支撑；研究针对网络情报信息实体及隐蔽关联的智能推理关键技术，实现网络空间情报信息推理图谱构建，支撑面向网络安全案事件与情报信息的复杂推理和隐蔽推理；研究基于战术博弈及战力储备的攻防潜能对抗关键技术，实现网络空间攻防对抗能力图谱构建，形成涵盖网络空间监测、评估、决策、反制的攻防潜能技术体系。

考核指标：形成多学科交叉、跨空间融合的新一代网络空间地理学理论体系，网络空间时空数据可视化表达模型不少于 15 个，构建不少于 10 大类的网络空间节点识别标签库，提出基于服务依赖性测度的特定目标脆弱性感知指标体系和验证方法，支持多类、多域跨层级依赖性测度及动态关系跨域关联，维度不少于 50 维；形成全球网络空间认知原型系统，涵盖 IPv4、IPv6、云和工业互联网等典型网络设施，发现稳定活跃地址不少于 5 亿以及不少于 8 万 BGP 前缀的 IPv6 活跃地址集合，实现对网络空间等级保护目标、关键信息基础设施保卫目标和重点威胁源的识别；研制智能推理与调查分析原型系统，构建面向网络安全保卫实战的情报图谱，支持文本类威胁情报信息的融合，实现能够支

撑情报信息挖掘、案事件侦查调查、重大活动网络安保等不少于4类网络安全保卫业务、12种分析推理算法或模型；构建网络空间技术对抗原型系统，实现未知威胁监测、攻防策略评估、装备能力评估、战力储备等技术储备，支持不少于4类、12种攻击行为的应急处置与技术对抗，形成网络技术对抗技战法模型库；支持在公安行业开展技术验证。

有关说明：由公安部组织推荐，配套经费与国拨经费不低于3:1。

关键词：网络空间地理图谱，网络空间保卫，技术对抗，非对称能力。

4 新技术新应用安全治理

4.1 工业生产控制软件安全分布式众测技术（共性关键技术类）

研究内容：针对互联网众测环境下的人员可信、行为可控、成果可验等需求，研究安全测试人员实人认证管控及信誉评价机制、众测平台恶意行为阻断机制、众测平台漏洞自动化验证机制等；突破工业生产控制软件测试的物理与空间限制，研究工业软件测试环境构建技术、工控系统/物联网设备硬件虚拟化技术、工业生产设备仿真模拟与虚实互联技术，实现虚实设备统一管理调度配置方法；研究众测平台环境下的测试用例筛选技术，突破工业软件安全众测平台的漏洞测试有效性增强技术。

考核指标：支持对X86/X86-64、ARM/ARM-64、MIPS、PowerPC等不少于6种处理器架构的虚拟化仿真，支持Windows、Linux、Android、FreeRTOS、VxWorks等不少于4种操作系统类

型虚拟化部署，实现不少于 100 种工控系统/工业物联网设备硬件的虚拟化仿真；支持设备状态数字化展示与虚实互联反馈，实现对数据采集与监控系统（SCADA）、分布式控制系统（DCS）等不少于 20 种工业控制系统软件的仿真模拟；支持在运行测试前有效过滤无法触发漏洞的测试用例，对无法触发漏洞的测试用例的过滤率不小于 50%，对于可触发漏洞的用例的留存率不小于 90%，千次识别耗时不超过 1 秒；支持基于工业软件特性和众测人员需求的辅助生成测试用例技术，提供 3 种以上的众测人员需求配置方式，使众测过程中使用辅助技术生成测试用例的效率和生成的测试用例可触发漏洞的比例对比未使用该技术的提升一倍；在不少于 4 个工业细分行业开展应用；制定相关国家、行业或团体技术标准不少于 3 项。

关键词：工业生产控制软件，分布式众测，硬件虚拟化，测试有效性增强。

4.2 智能驾驶系统融合安全防护与测试关键技术（共性关键技术类）

研究内容：针对智能驾驶系统缺少功能安全与网络安全一体化保障手段、大规模应用面临多种未知攻击和严峻安全威胁的问题，研究智能驾驶系统多层级网络与终端融合安全设计方法，突破基于系统软硬件漏洞及隐蔽后门的未知网络攻击检测技术，研发智能驾驶系统融合安全防护功能模块，突破智能驾驶信息物理系统功能安全和网络安全一体化保障技术，建立智能驾驶系统多

层级网络与终端融合安全测试验证平台，并在多种场景下开展智能驾驶系统融合安全关键技术验证与示范应用。

考核指标：构建面向智能驾驶系统多层级网络与终端的融合安全技术体系，可识别网络攻击不低于20种，类型覆盖DDoS、提权、伪装、终端环境感知欺骗、控制劫持等常见网络攻击及未知网络攻击，平均准确率不低于98%，平均误报率不高于5%；融合安全防护功能模块具备智能驾驶核心算法、存储数据、运行机制的主动隐匿和动态调节等功能；融合安全测试验证平台包含漏洞库、测试工具库、测试规范集等模块，支持测试环境虚拟化，支持特权升级、注入、渗透、预置后门、感知欺骗、控制劫持等可用性及安全性测试，攻防测试方式不少于20种，并具备攻击链可视化功能；智能驾驶系统融合安全技术与测试验证平台示范应用场景不少于3类；制定相关国家、行业或团体技术标准不少于3项。

关键词：智能驾驶系统，融合安全，功能安全和网络安全一体化保障。

4.3 高可靠实时互联的工业无线网络安全关键技术（共性关键技术类）

研究内容：针对智能制造无线互联与安全关键工业领域高安全本质要求的矛盾，研究工业无线网络安全风险传播途径和传播机理，建立基于知识图谱的工业无线网络威胁感知、风险分析与攻击链阻断方法；研究工业无线测控设备物理特征的提取、呈现

和度量机制，设计基于设备物理特征的身份认证、时变密钥生成及一致性校验等链路层安全防护技术；研究基于可信数据链的分布式共识机制、加密机制、数据共享和完整性保障技术，构建基于分布式可信数据链的工业无线网络安全一体化防护技术体系；研制工业无线网络安全射频芯片、安全通信与监测设备及全生命周期安全管控系统，在安全关键领域典型智能制造车间开展应用验证。

考核指标：建立面向制造装备互联的内嵌式工业无线网络安全技术体系，能够检测和防御数据破解、链路监听、通信干扰、报文伪装等 4 大类风险不少于 10 种，检测准确率达到 95%以上，在保证安全前提下，百点规模网络达到 99.99%可靠性，时延不大于 20ms；研制自主可控的安全无线射频芯片及协议栈 1 套、工业无线网络安全通信与监测设备不少于 5 种、全生命周期安全管控软件 1 套，搭建工业无线网络安全攻防实验平台；在典型安全关键行业的应用验证不少于 3 项，其中，在军工领域应用验证不少于 1 项；制定相关国家、行业或团体技术标准不少于 1 项。

有关说明：申报单位及参研单位应具备相应资质，具有军工无线技术应用经验的单位优先。

关键词：智能制造装备，工业无线网络，全生命周期安全。

4.4 支撑海量终端接入与跨安全域协同的云安全防御关键技术研究（共性关键技术类）

研究内容：本项目针对能源、制造等重点行业产业链上下游

通过多云/云边跨域协同带来的多业务主体安全水平不一、身份难鉴别、威胁易扩散、数据易泄露等问题，围绕关键基础设施产业链多业务主体的跨域安全协同场景，研究多云/云边协同的创新计算模式和网络安全体系，实现多主体业务、数据、资源协同与安全防护统一管理；研究自主可控、安全可信的云基础设施关键技术，形成支持云边端多维协同的安全基础设施；研究面向边缘设施的轻量级密码和安全检测技术，构建边缘弱算力环境下的云边安全通信机制，实现高效的终端可信接入与可靠的云边数据协同；研究分布式资源协同网络多点跨域服务网络安全监测和主动防御关键技术，构建覆盖多云/云边的网络安全协同防御体系；基于能源、制造等重点行业关键信息基础设施开展跨域资源协同的云安全示范应用。

考核指标：制定支持跨异构云平台、跨数据中心、多站融合、云边协同等环境的分布式资源协同网络安全体系，形成国际/国家标准提案 1 项；支持云边协同业务场景不少于 4 项；构造面向边缘弱算力环境的轻量级密码算法和安全检测能力，接入身份认证运算处理能力不小于 10000 次/秒，接入加密处理能力不小于 20000 次/秒，实现安全、可靠、高效的云边数据协同；实现跨域网络终端、节点的安全统一监测，单一代理（Agent）能够实现对硬件服务器、虚拟机、容器各类工作负载进行统一管控，处理器资源占用不超过 50%，完成不少于 5 种典型多云/云边协同场景下的安全防护和隔离应用验证；与现网环境对比，同等攻击场景下，

攻击者通过边缘主机横向移动到内部靶标主机的时间成本增加3倍，内部暴露端口数减少50%，东西向攻击面减少30%；支持能源、制造等重点行业示范应用场景不少于3种，接入终端类型不少于10种，接入数量不少于50万。

关键词：多云/云边协同，云安全，防御，隔离。

“网络空间安全治理”重点专项
2023 年度“揭榜挂帅”榜单

为深入贯彻落实国家科技创新有关部署安排，切实加强创新链和产业链对接，“网络空间安全治理”重点专项聚焦国家战略亟需、应用导向鲜明、最终用户明确的重大攻关需求，凝练形成 2023 年度“揭榜挂帅”榜单，现将榜单任务及有关要求予以发布。

一、申报说明

本批榜单拟启动 1 个项目，共拟安排国拨经费不超过 2200 万元。项目下设课题数不超过 5 个，项目参与单位总数不超过 10 家。项目设 1 名负责人，每个课题设 1 名负责人。

榜单申报“不设门槛”，项目牵头申报和参与单位无注册时间要求，项目（课题）负责人无年龄、学历和职称要求。申报团队数量不多于拟支持项目数量的榜单任务方向，仍按程序进行项目评审立项。明确榜单任务资助额度，简化预算编制，经费管理探索实行“负面清单”。

二、攻关和考核要求

揭榜立项后，揭榜团队须签署“军令状”，对“里程碑”考核要求、经费拨付方式、奖惩措施和成果归属等进行具体约定，并将榜单任务目标摆在突出位置，集中优势资源，全力开展限时攻关。项目（课题）负责人在揭榜攻关期间，原则上不得调离或辞

去工作职位。

项目实施过程中，将最终用户意见作为重要考量，通过实地勘察、仿真评测、应用环境检测等方式开展“里程碑”考核，并视考核情况分阶段拨付经费，实施不力的将及时叫停。

项目验收将通过现场验收、用户和第三方测评等方式，在真实应用场景下开展，并充分发挥最终用户作用，以成败论英雄。由于主观不努力等因素导致攻关失败的，将按照有关规定严肃追责，并依规纳入诚信记录。

三、榜单任务

1. 油气管网控制系统跨域多维安全智能预警关键技术（共性关键技术类）

研究内容：在国家油气输送“全国一张网”的发展格局下，针对油气管网生产调度数据采集与监视系统覆盖全国、广域互联、跨域联动的特点，分析油气管网面临的多源网络安全威胁与管道本体及生产设施运行风险影响因素，研究网络攻击渗透与管网系统物理破防内在因果机理；研究广域集中调控模式下，海量数据的完整性和机密性保护技术以及网络可信接入技术和动态安全防护机制；研究融合信息安全和功能安全的跨域远控分布式场站本质安全技术与数据采集与监控系统（SCADA）内生防御主动安全策略；研究油气管网控制系统多维安全融合风险预警与智能决策技术，研制广域多维安全风险态势感知与智能安全管控平台；研究广域大系统安全仿真测试技术，构建油气管网多维安全一体化

测试验证平台。

考核指标：研制广域多维安全风险态势感知与智能安全管控平台，具备多源异构现场数据接入、融合功能安全和信息安全技术的实时一体化风险评估、智能预警、分级决策等功能，支持至少 6 类工业数据协议，攻击事件发现到报警或隔离响应时间不超过 200ms，误报率不超过 5%，在国家油气管网完成现场应用验证。研制油气管网多维安全一体化测试验证平台，具备攻击渗透时空演化与管网物理破防内在机理、跨域安全融合等关键技术验证能力，在国家油气管网完成现场应用验证。申请发明专利不少于 3 项，制定相关国家、行业或团体技术标准不少于 2 项。

有关说明：由企业牵头申报，配套经费与中央财政经费比例不低于 3:1。研发时限为 3 年，立项 1 年和 2 年后开展“里程碑”考核。

榜单金额：不超过 2200 万元。

关键词：多维安全，智能预警，风险态势感知，油气管网。

"网络空间安全治理"重点专项 2023 年度
项目申报指南和榜单形式审查条件要求

申报项目须符合以下形式审查条件要求。

1. 推荐程序和填写要求

（1）由指南规定的推荐单位在规定时间内出具推荐函。

（2）申报单位同一项目须通过单个推荐单位申报，不得多头申报和重复申报。

（3）项目申报书（包括预申报书和正式申报书，下同）内容与申报的指南方向相符。

（4）项目申报书及附件按格式要求填写完整。

2. 申报人应具备的资格条件

（1）项目（课题）负责人应为 1963 年 1 月 1 日以后出生，具有高级职称或博士学位。

（2）青年科学家项目负责人应具有高级职称或博士学位，男性应为 38 周岁以下（1985 年 1 月 1 日以后出生），女性应为 40 周岁以下（1983 年 1 月 1 日以后出生）。原则上团队其他参与人员年龄要求同上。

（3）受聘于内地单位的外籍科学家及港、澳、台地区科学家可作为项目（课题）负责人，全职受聘人员须由内地聘用单位提供全职聘用的有效材料，非全职受聘人员须由双方单位同时提供

聘用的有效材料，并作为项目预申报材料一并提交。

（4）参与重点专项实施方案或本年度项目指南编制的专家，原则上不能申报该重点专项项目（课题）。

（5）诚信状况良好，无在惩戒执行期内的科研严重失信行为记录和相关社会领域信用“黑名单”记录。

（6）中央和地方各级国家机关的公务人员（包括行使科技计划管理职能的其他人员）不得申报项目（课题）。

（7）项目申报人员满足申报查重要求。

3. 申报单位应具备的资格条件

（1）在中国大陆境内登记注册的科研院所、高等学校和企业等法人单位。国家机关不得作为申报单位进行申报。

（2）注册时间在2022年6月30日前。

（3）诚信状况良好，无在惩戒执行期内的科研严重失信行为记录和相关社会领域信用“黑名单”记录。

4. 本重点专项指南规定的其他形式审查条件要求

（1）“揭榜挂帅”项目（课题）负责人无年龄、学历和职称要求，项目牵头申报和参与单位无注册时间要求。

（2）青年科学家项目不再下设课题，项目参与单位总数不超过3家。

本专项形式审查责任人：张炜